

Catalyst 9800 WLC의 CAPWAP 킵얼라이브에 대한 이해 및 문제 해결

목차

[소개](#)

[컨텍스트](#)

[2개의 개별 채널, 2개의 서로 다른 메커니즘](#)

[CAPWAP 재전송](#)

[통합 타이머 참조](#)

[나란한 차이점](#)

[메커니즘별 RA 추적 로그 문자열](#)

[예:](#)

[작업 시나리오](#)

[CAPWAP 제어 패킷 검증\(UDP 포트 5246\)](#)

[CAPWAP 데이터 킵얼라이브 검증\(UDP 포트 5247\)](#)

[AP 업링크 스위치에서 삭제되는 제어 패킷\(UDP 5246\)](#)

[AP 업링크 스위치에서 삭제되는 CAPWAP 데이터 포트\(UDP 5247\)](#)

[CAPWAP 데이터 킵얼라이브 비활성화](#)

소개

이 문서에서는 CAPWAP 컨트롤 킵얼라이브, 데이터 킵얼라이브 및 재전송,

컨텍스트

CAPWAP는 Cisco Catalyst 9800 플랫폼의 Cisco 액세스 포인트와 무선 LAN 컨트롤러 간의 통신 프레임워크를 제공합니다. 연결을 유지하기 위해 정의된 keepalive 및 재전송 메커니즘과 함께 별도의 제어 및 데이터 채널을 사용합니다.

이 문서에서는 CAPWAP 제어 킵얼라이브, 데이터 킵얼라이브 및 재전송에 대해 설명하며, 여기에는 관련 타이머, 장애 동작 및 주요 문제 해결 지표가 포함됩니다.

2개의 개별 채널, 2개의 서로 다른 메커니즘

CAPWAP는 두 개의 UDP 채널을 통해 실행되며, 각각 라이브니스 메커니즘이 있습니다

채널	기본 포트(UDP)	라이브니스 메커니즘
제어	5246	에코 요청/에코 응답
데이터	5247	데이터 채널 연결 유지

CAPWAP 제어 킵얼라이브(에코/하트비트)

목적

CAPWAP 제어 킵얼라이브는 액세스 포인트가 제어 채널에 여전히 연결 가능한지 확인하는 데 사용됩니다.

그 목적은 매우 간단합니다. 또한 AP와 컨트롤러 간의 제어 연결이 여전히 활성 상태이며 응답하는지 확인합니다. 컨피그레이션 업데이트 또는 클라이언트 데이터를 전달하는 데 사용되지 않습니다. 대신 UDP 포트 5246을 통한 CAPWAP 제어 경로에 대한 라이브니스 메커니즘 역할을 합니다.

누가 킵얼라이브를 보내죠?

액세스 포인트는 제어 킵얼라이브를 능동적으로 시작하는 디바이스입니다.

필요한 경우 AP가 컨트롤러에 CAPWAP 에코 요청을 보냅니다. 그러면 컨트롤러는 해당 에코 응답으로 응답합니다. 이러한 응답은 제어기가 요청을 수신하였고 제어 채널이 양방향으로 기능함을 확인한다.

응답은 요청과 일치하며, 이를 통해 AP는 전송한 keepalive에 대한 유효한 응답을 수신하는지 확인할 수 있습니다.

이 동작은 제어 킵얼라이브가 주로 컨트롤러 구동 폴링 메커니즘이 아님을 보여주기 때문에 중요합니다. 대신 AP가 제어 채널 연결성을 확인하고 컨트롤러가 이에 따라 응답합니다.

에코 간격은 고정된 일정이 아니라 비활성 상태를 기반으로 합니다

이는 CAPWAP 컨트롤 keepalive에서 가장 일반적으로 잘못 이해되는 부분 중 하나입니다.

일반적인 가정은 AP가 고정된 주기적 하트비트처럼 30초마다 에코 요청을 전송한다는 것입니다. 실제로는 그렇게 되지 않습니다.

제어 킵얼라이브는 제어 채널 비활성을 기반으로 합니다. 이는 제어 채널이 구성된 간격 동안 유휴 상태일 때만 AP가 독립형 에코 요청을 전송함을 의미합니다. AP와 컨트롤러 간에 다른 제어 트래픽이 이미 교환되고 있는 경우 별도의 에코 패킷을 보낼 필요가 없습니다.

AP와 컨트롤러 사이의 모든 유효한 제어 통신은 제어 채널이 살아있음을 효과적으로 증명한다. 따라서 일반 CAPWAP 제어 트래픽은 keepalive 타이머를 재설정합니다.

이러한 제어 트래픽의 예는 다음과 같습니다.

- 컨피그레이션 교환
- 무선 리소스 관리 업데이트
- WLAN 관련 제어 메시지
- 클라이언트 관련 제어 이벤트
- 통계 또는 상태 동기화 메시지
- 정상 작업의 일부로 교환되는 기타 CAPWAP 제어 패킷

그 결과, 독립형 에코 요청은 제어 채널이 조용하지 않은 기간에만 표시됩니다.

간단한 예

show capwap client timer 명령을 사용하여 AP의 CAPWAP 에코 타이머를 확인할 수 있습니다.

<#root>

Training-AP#

show capwap client timer

CAPWAP TIMERS Running Current / Max (seconds)

PATHMTU_TIMER : 23 / 30

MSG_CLIENT_STAT : 124 / 180

DATA_CHANNEL_KEEP_ALIVE_TIMER : 24 / 30

ECHO_INTERVAL_TIMER : 23 / 30

PERIODIC_ECHO_TIMER : 233 / 300

PRIMARY_DISCOVERY_TIMER : 50 / 120

CAPWAP_WDG_UPDATE_TIMER : 4 / 5

FLASH_WRITE_INTERVAL_TIMER : 21 / 60

타이머

제어 킵얼라이브 메커니즘은 두 개의 중요한 타이밍 값에 의존한다.

항목	기본 값	설명
에코 간격	30초	AP가 독립형 에코 요청을 보내기 전의 제어 채널 비활성 상태 양입니다
컨트롤러 제어 데드 타이머	90초	제어 세션 데드를 선언하기 전에 컨트롤러가 유효한 제어 트래픽을 수신하지 않고 허용하는 최대 시간

컨트롤 Keepalive 실패 시 수행되는 작업

제어 채널이 허용된 시간 초과 동안 무음으로 전환되면 컨트롤러는 결국 제어 세션이 손실됨을 선언합니다.

이 시점에서 컨트롤러는 AP가 더 이상 제어 채널에 연결할 수 없는 것으로 간주하고 세션 해제를 시작합니다. 여기에는 일반적으로 제어 연결을 닫고 AP의 활성 제어 세션 상태를 제거하는 것이 포함됩니다.

그런 다음 AP는 장애 시나리오에 따라 컨트롤러를 다시 검색하고 다시 연결하여 연결을 다시 설정하려고 시도할 수 있습니다.

문제 해결 관련 사항

이 keepalive 동작을 이해하는 것은 트러블슈팅 과정에서 필수적입니다.

에코 패킷이 누락되었다고 해서 항상 문제가 되는 것은 아닙니다

패킷 캡처에 30초마다 에코 요청이 표시되지 않으면 자동으로 결함이 나타나지 않습니다. 이는 다른 CAPWAP 제어 트래픽이 충분히 흐르고 있음을 의미할 수 있으므로 독립형 에코가 필요하지 않습니다.

불규칙한 에코 간격은 일반적으로 정상입니다.

에코는 비활성 상태에 의해 트리거되므로 종종 불균일한 간격으로 나타납니다. 이는 정상적인 동작입니다.

전반적인 제어 채널 활동에 주력

AP 연결 끊김을 트러블슈팅할 때 다음 사항을 묻는 것이 더 유용합니다.

- 컨트롤러가 AP로부터 CAPWAP 제어 트래픽을 계속 수신합니까?
- 제어 채널은 데드 타이머를 작동시킬 만큼 오랫동안 무음인가?
- 제어 경로에만 영향을 주는 네트워크 문제가 있습니까?
- 패킷 손실, 방화벽 동작, NAT 문제 또는 컨트롤 플레인 삭제로 인해 UDP 5246 트래픽이 중단됩니까?

실제 문제는 주기적인 에코 패킷 자체가 없는 것이 아닙니다. 실제 문제는 컨트롤러가 AP에 연결할 수 없다고 선언할 정도로 오랫동안 제어 채널 통신이 끊어지는 것입니다.

CAPWAP 데이터 킥얼라이브

목적

CAPWAP 제어 에코는 제어 채널이 작동하고 있음을 확인하지만, 데이터 채널 또한 정상임을 증명하지 않는다. 제어 경로 및 데이터 경로는 독립적으로 실패할 수 있으므로 CAPWAP는 UDP 포트 5247에서 별도의 데이터 keepalive를 사용합니다.

데이터 킥얼라이브의 목적은 다음과 같습니다.

- ap가 데이터 채널의 컨트롤러에 계속 연결할 수 있는지 확인합니다
- AP의 데이터 터널 상태 유지
- 데이터 경로에만 영향을 주는 장애 탐지

누가 전송하는지, 컨트롤러는 어떻게 반응하는지

AP가 데이터 킥얼라이브를 전송하고, 컨트롤러가 데이터 킥얼라이브 응답으로 응답합니다.

응답은 데이터 채널 암호화가 활성화되었는지 여부에 따라 암호화되거나 암호화되지 않을 수 있습니다.

keepalive가 유효한 경우 컨트롤러는 이를 사용하여 AP의 데이터 경로에 계속 연결할 수 있는지 확인합니다. 패킷을 유효한 AP 세션과 일치시킬 수 없거나 응답을 보낼 수 없는 경우, keepalive가 삭제되고 데이터 경로가 결국 실패한 것으로 간주될 수 있습니다.

컨트롤러가 검증하는 방법

keepalive를 수락하기 전에 컨트롤러는 기본 검증을 수행하여 패킷이 올바른 AP에 속하는지 확인합니다.

컨트롤러는 다음을 확인합니다.

- keepalive에 유효한 CAPWAP 정보가 포함되어 있습니다.
- ap 무선 MAC 주소가 있습니다.
- 패킷을 AP 세션과 일치시킬 수 있습니다

컨트롤러는 먼저 소스 IP 주소 및 소스 UDP 포트를 사용하여 세션을 식별하려고 시도합니다. 실패할 경우 AP 라디오 MAC 주소를 다시 사용할 수 있습니다.

이는 데이터 채널이 제어 채널과는 다른 변환된 UDP 포트에서 올 수 있는 NAT 또는 PAT 뒤의 AP에 중요합니다. 이러한 경우 컨트롤러는 AP의 실제 데이터 채널 튜플을 학습하고 업데이트할 수 있습니다.

패킷이 해당 IP 포트 조합과 이미 연결된 세션이 아닌 다른 AP에 속한 것으로 나타나면 잘못된 세션 매핑을 방지하기 위해 keepalive가 거부됩니다.

검증 후 수행되는 작업

keepalive가 수락되면 컨트롤러는 AP의 현재 세션 상태를 기반으로 이를 처리합니다.

- 데이터 세션이 이미 설정된 경우, keepalive는 단순히 라이브성을 새로 고칩니다.
- 이것이 첫 번째 유효한 데이터 킵얼라이브인 경우 컨트롤러는 이를 사용하여 AP의 데이터 채널 정보를 학습하거나 업데이트하고 데이터 터널 설정을 완료할 수 있습니다.

이 첫 번째 킵얼라이브는 AP가 NAT 또는 PAT 뒤에 있는 경우를 포함하여 컨트롤러가 데이터 터널을 올바르게 프로그래밍하는 데 도움이 되므로 특히 중요합니다.

데이터 세션이 완전히 설정되면 향후 keepalive는 정상적인 정상 상태 경로를 따르며 라이브성을 유지하기 위해서만 사용됩니다.

중요한 행동

유효한 데이터 keepalive는 데이터 경로의 상태를 확인하는 것 이상을 수행합니다. 컨트롤러에서 AP의 전체 세션 라이브도 새로 고칩니다.

즉, 컨트롤러에서 데이터 채널 라이브니스가 전체 AP 세션 상태에 기여합니다. 그 결과, 제어 및 데이터 라이브니스 메커니즘은 서로 다른 목적을 제공함에도 불구하고 서로 관련되어 있다.

AP측 데이터 킵얼라이브 타이머

AP는 데이터 킵얼라이브 간격을 제어하고 데이터 터널이 중단된 것으로 간주해야 하는 시기를 결정합니다.

항목	기본값
데이터 킵얼라이브 간격	30초
재전송 백오프	3초, 6초, 12초, 15초
데이터 데드 간격	180초

정상 상태에서 AP는 30초마다 데이터 킵얼라이브를 전송합니다.

AP가 응답을 받지 못하면 백오프 패턴을 사용하여 재시도합니다. 장애가 180초 동안 지속되면 AP는 데이터 터널 다운을 선언합니다.

CAPWAP 재전송

핵심 원리: 신뢰성은 양방향으로 작동함

CAPWAP 제어 메시징은 UDP를 통해 실행되더라도 요청 및 응답 모델을 사용합니다. 신뢰성을 제공하기 위해 요청을 보내는 장치도 예상 응답을 수신할 때까지 이를 재전송할 책임이 있습니다.

이는 재전송이 대칭적임을 의미합니다.

- 컨트롤러가 AP에 요청하는 경우(예: 컨피그레이션 업데이트), 컨트롤러는 재전송을 처리합니다.
- 검색, 가입, 컨피그레이션 상태, 이미지 관련 메시지 및 에코 요청과 같은 AP에서 컨트롤러에 대한 요청의 경우 AP는 재전송을 처리합니다.

이는 중요한 트러블슈팅 포인트입니다. 패킷 캡처에서 AP-컨트롤러 재전송이 표시되는 경우, 이는 일반적으로 AP가 예상 응답을 받지 못했기 때문에 단순히 자체 요청을 재시도하고 있음을 의미합니다. 이는 가입 중에 정상이며 제어 에코 활동 중에 발생할 수도 있습니다.

컨트롤러측 재전송 동작

컨트롤러에서 재전송은 전용 전송 신뢰성 상태 머신에 의해 처리됩니다.

간단히 말해 컨트롤러는 다음을 수행합니다.

1. 승인이 필요한 요청을 수락합니다.
2. AP별 전송 큐에 넣습니다.
3. 요청을 보냅니다.
4. 일치 응답을 기다립니다.
5. 응답이 도착하면 큐에서 제거하거나 타이머가 만료되면 다시 전송합니다.

이 로직은 각 AP 세션에 대해 개별적으로 추적됩니다. 컨트롤러는 또한 전송 윈도우 및 미처리 요청 메시지의 수를 유지합니다.

컨트롤러가 재전송 여부를 결정하는 방법

재전송 타이머가 만료될 때마다 컨트롤러는 대기열에 있는 요청 항목을 검토하고 다음 결정 중 하나를 수행합니다.

1. 응답이 이미 잘못 수신되었습니다.

해당 요청에 대한 응답이 이미 수신된 경우, 해당 응답이 비순차적으로 도착하더라도 컨트롤러는 메시지를 다시 전송하지 않습니다.

2. 재시도 제한 초과

요청이 이미 허용된 횟수 이상 재전송된 경우 컨트롤러는 이를 실패로 간주하고 해당 AP 세션에 대한 전송 프로세스를 중단합니다.

이 시점에서 AP 세션이 종료됩니다.

3. 요청이 아직 오래되지 않았습니다.

컨트롤러는 모든 타이머 이벤트에서 대기열에 있는 모든 메시지를 즉시 재전송하지 않습니다. 요청이 다시 전송되기 전에 최소한 재전송 간격 동안 대기열에 남아 있어야 합니다.

기본적으로 이 재전송 간격은 3초입니다.

4. 요청 재전송

요청이 아직 보류 중이고, 시간이 충분히 경과했으며, 재시도 제한을 초과하지 않은 경우 컨트롤러는 CAPWAP 제어 채널에서 요청을 재전송하고 재시도 카운터를 늘립니다.

특별한 경우: 유선 데이지 체인 AP

유선 데이지 체인 AP 경로를 사용하는 메시 구축의 경우 컨트롤러는 더 많은 재시도 예산을 허용합니다.

이 경우, 정상 재시도 한도는 효과적으로 3배 증가합니다.

기본 재시도 횟수 5를 사용하면 컨트롤러가 실패를 선언하기 전에 최대 15번 재시도할 수 있습니다.

이러한 토폴로지는 지연 또는 메시지 손실에 대해 더 많은 허용 범위를 요구할 수 있으므로 이 예외가 있습니다.

AP 측 재전송 동작

AP는 자체 CAPWAP 요청도 재전송하지만 컨트롤러와 다른 패턴을 사용합니다.

컨트롤러가 고정 재전송 간격을 사용하는 동안 AP는 지수 백오프를 사용합니다. 즉, 각 실패 시도 후 대기 시간이 증가합니다.

기본 설정에서는 AP 재시도 타이밍이 대략 다음과 같습니다.

- 6초
- 12초
- 24초
- 48초
- 96초

이 동작은 다음과 같은 AP 시작 CAPWAP 요청에 적용됩니다.

- 검색
- 참가
- 설정 관련 거래소
- 암호화된 제어 트랜잭션
- 에코 요청

이러한 재시도 매개변수는 AP 조인 컨피그레이션의 일부로 컨트롤러에서 학습됩니다.

패킷 캡처의 진단 핑거프린트

재전송 패턴 자체는 문제 해결 중에 유용한 단서가 되는 경우가 많습니다.

재전송 패턴	유력한 출처
균일한 간격의 재전송, 약 3초 간격	컨트롤러측 재전송
6s, 12s, 24s, 48s, 96s와 같이 시간이 지남에 따라 더 멀리 확산되는 재전송	지수 백오프를 사용하는 AP측 재전송

이는 특히 참가 실패 또는 에코 관련 문제 중에 어떤 쪽이 재시도되고 있는지 확인할 수 있는 실용적인 방법입니다.

재시도 횟수 초과 시 수행되는 작업

기대했던 응답을 받지 못한 채 재전송이 이어지면 결국 양쪽 모두 포기하지만 복구 행동은 다르다.

컨트롤러측

컨트롤러에서 재시도 예산을 소진하면 전송 프로세스가 중단되고 AP 세션이 종료됩니다. 그러면 CAPWAP 컨트롤 및 데이터 세션이 닫힙니다.

AP 측

AP에서 자체 재시도 시도를 소진하는 경우 해당 컨트롤러를 포기하고 처음부터 다시 시작합니다. 일반적으로 Discovery(검색) 단계로 돌아가 전체 재조인을 시도합니다.

컨피그레이션 노브 및 기본값

재전송 동작은 AP 조인 프로파일의 두 가지 기본 설정에 의해 제어됩니다.

명령을 사용합니다	기본값	기능
capwap 재전송 횟수	5	최대 재전송 시도 횟수
capwap 재전송 간격	3초	기본 재전송 간격

이러한 값은 조인 신뢰도와 에코 관련 재시도를 비롯한 기타 AP 기반 CAPWAP 제어 재시도에 모두 영향을 미칩니다.

통합 타이머 참조

이 표에서는 이 문서에서 논의된 주요 CAPWAP 타이머를 요약합니다.

타이머	기본값	평면	소유자	설명
에코 간격 제어	30초	제어	AP	AP가 30초 동안 CAPWAP 제어 트래픽을 전송하지 않으면 에코 요청을 보냅니다.
하트비트 데드 타이머 제어	90초	제어	컨트롤러	컨트롤러에는 이 창 내에서 유효한 제어 트래픽이 필요합니다. 아무것도 수신되지 않으면 제어 세션이 중단된 것으로 간주됩니다.
재전송 간격 제어	3초	제어	컨트롤러	컨트롤러가 자체 미응답 CAPWAP 요청을 고정 간격으로 재전송합니다.
재전송 횟수 제어	5회 시도	제어	컨트롤러	컨트롤러 시작 CAPWAP 요청에 대한 최대 재시도 횟수입니다. 유선 데이터 체인 시나리오에서는 15회 시도까지 늘어날 수 있습니다.
AP 제어 재전송 백오프	6, 12, 24, 48, 96초	제어	AP	AP는 지수 백오프를 사용하여 자체 CAPWAP 요청을 재전송합니다.
데이터 킵얼라이브 간격	30초	데이터	AP	정상 상태에서 AP는 30초마다 데이터 킵얼라이브를 전송합니다.
데이터 킵얼라이브 재시도 백오프	3, 6, 12, 15, 15초	데이터	AP	데이터 킵얼라이브 응답이 누락되면 AP는 백오프를 사용하여 15초로 제한하여 재시도합니다.
데이터 채널 데드 간격	180초	데이터	AP	AP가 이 기간 내에 데이터 킵얼라이브 교환을 성공적으로 유지하지 못하면 데이터 터널 다운을 선언합니다.

나란한 차이점

킵얼라이브 vs. 재전송

때때로 혼동되기도 하지만 keepalive와 재전송은 서로 다른 목적을 제공합니다.

양상	킵얼라이브	재전송
주요 목적	피어에 계속 연결할 수 있는지 확인합니다.	응답이 수신되지 않을 때 특정 요청을 재시도합니다.
범위	세션당 또는 채널당	메시지당
트리거	비활성 또는 라이브니스 시간 초과	요청이 응답하지 않습니다.
추적 방법	시간 기반	재시도 횟수 기반
실패의 의미	채널 또는 세션에 더 이상 연결할 수 없습니다.	특정 CAPWAP 교환이 반복적으로 실패했습니다.
실패 결과	세션을 아래로 선언할 수 있음	컨트롤러가 세션을 종료하거나 AP가 조인을 다시 시작할 수 있음

메커니즘별 RA 추적 로그 문자열

AP별 추적을 위해 AP에 대한 로그를 수집하고 이러한 정확한 문자열을 검색합니다.

로그 수집

Use:

- 무선 mac 디버그 <ap-radio-mac>
- show logging profile 무선 필터 mac <ap-radio-mac> to-file bootflash:<file>

keepalive/하트비트 제어

검색 대상:

- 에코 요청 처리
- 에코 응답 구축
- 시퀀스 번호가 <N>인 요청에 대해 에코 응답이 전송되었습니다.
- 하트비트 타이머가 새 값 <ms>로 다시 시작되었습니다.
- 하트비트 타이머 터치가 호출됨
- 하트비트 타이머 만료

데이터 연결 유지

검색 대상:

- 데이터 킵얼라이브 수신됨
- 데이터 세션이 이미 설정됨
- 데이터 DTLS가 설정되지 않았습니다.
- CAPWAP 데이터 터널 항목 업데이트
- 데이터 킵얼라이브를 처리하지 못했습니다. 이유: CAPWAP 세션이 실행 또는 구성 상태가 아닙니다.
- 잘못된 keepalive 메시지, capwap 블록 없음
- 잘못된 keepalive 메시지, WTP MAC 없음
- 킵얼라이브를 처리하지 못했습니다. CAPWAP 세션을 찾을 수 없습니다.
- 제어 포트가 아닌 다른 포트에서 데이터 유지 관리가 수신됩니다. <포트>
- 다른 AP <mac>에 대해 데이터 연결 유지 수신
- 원격 호스트에 대한 WTP 세션 테이블에서 데이터 튜플 정보를 업데이트하지 못했습니다. <ip>
- CAPWAP 데이터 터널 항목을 업데이트하지 못했습니다.

데이터 플레인 킵얼라이브 처리

검색 대상:

- <src>에서 <dst>(으)로 데이터 연결 유지
- <enc/plain> 데이터 연결 유지 응답 보냄
- IP에서 킵얼라이브 패킷 삭제: <ip>, 알 수 없는 세션
- IP에서 킵얼라이브 패킷 삭제: <ip>, 데이터 DTLS 상태를 가져오지 못했습니다.
- 데이터 킵얼라이브 응답을 보내지 못했습니다.
- 로드 밸런싱 데이터 킵얼라이브 메시지 실패

재전송

검색 대상:

- 재전송 타이머 콜백
- Seqnum <N>이(가) 큐에 있지만 아직 ack를 받지 못했으므로 다시 전송하는 중입니다.
- 메시지 재전송: <msg-name> 재전송 시도: <M>
- 시퀀스 번호가 있는 항목: <N>이(가) <S>초 동안 대기열에 있습니다. 재전송 안 함
- CAPWAP 세션 종료, 최대 재전송 만료: <메시지> ...
- AP에서 CAPWAP 세션 리소스를 정리합니다.

세션 해체

검색 대상:

- AP CAPWAP 세션을 종료합니다.
- CAPWAP DTLS 세션을 닫습니다.
- capwap-dtls 제어 세션 닫기
- capwap-dtls 데이터 세션 닫기
- <S>초 전에 마지막으로 수신된 제어 패킷입니다.
- <S>초 전에 수신된 마지막 데이터 연결 유지 패킷입니다.
- AP에 대해 CAPWAP DTLS 세션이 닫혔습니다. 원인: <이유>

예:

작업 시나리오

AP 디버그 확인

이 AP 디버그 명령은 AP와 WLC 간의 CAPWAP 제어 및 데이터 킵얼라이브 통신을 모니터링하는데 사용할 수 있습니다.

```
#debug capwap client event
```

이러한 디버그 로그는 성공적인 CAPWAP 통신 시퀀스를 보여줍니다.

13:11:44에 AP가 UDP 포트 5246을 통해 WLC에 CAPWAP 에코 요청을 전송했습니다. 동일한 간격 동안 AP는 UDP 포트 5247을 통해 CAPWAP 데이터 킵얼라이브 패킷도 전송했습니다. 로그는 WLC가 두 요청에 모두 성공적으로 응답했음을 확인합니다.

타임스탬프는 일반적인 CAPWAP 통신 주기를 나타냅니다.

- 13:11:44.0917 - 에코 요청이 전송되었습니다.
- 13:11:44.0918 - 데이터 킵얼라이브가 전송되었습니다.
- 13:11:44.0926 - 데이터 킵얼라이브가 WLC에서 수신되었습니다.
- 13:11:44.0940 - WLC에서 에코 응답을 받았습니다.

이러한 타임스탬프는 CAPWAP 컨트롤 및 데이터 채널이 모두 예상대로 작동하며 왕복 지연 시간이 거의 없음을 확인합니다.

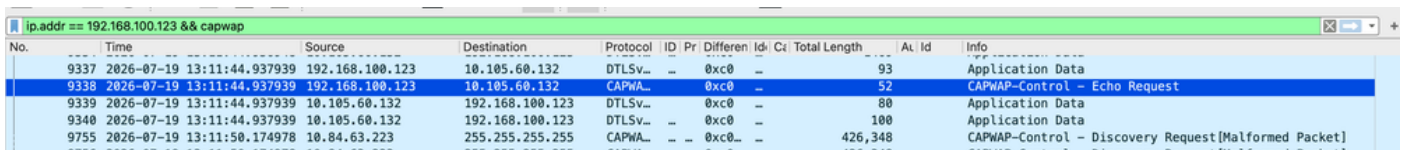
```
[*07/19/2026 13:11:14.0817] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/19/2026 13:11:44.0917] Echo Request: Send count 22
[*07/19/2026 13:11:44.0917] [TX]Echo Request: Sent to 10.105.60.132
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 13:11:44.0918] [TX]KEEPALIVE: Schedule for Retransmit in 3 sec sec_drop_count=0
[*07/19/2026 13:11:44.0918] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 13:11:44.0926] chatter: [RX]KEEPALIVE: Count 164
[*07/19/2026 13:11:44.0927] Sending KEEPALIVE to WTP SM
[*07/19/2026 13:11:44.0927] Capwap data keep-alive Msg.
[*07/19/2026 13:11:44.0927] [RX]KEEPALIVE: Session ID 3221108139, Next scheduled for TX in 30 sec
[*07/19/2026 13:11:44.0927] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/19/2026 13:11:44.0940] [RX]Echo Response from 10.105.60.132
[*07/19/2026 13:11:44.0004] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 13:12:14.0004] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 13:12:14.0005] [TX]KEEPALIVE: Schedule for Retransmit in 3 sec sec_drop_count=0
[*07/19/2026 13:12:14.0005] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
```

CAPWAP 제어 패킷 검증(UDP 포트 5246)

패킷 캡처 분석

패킷 캡처는 AP가 UDP 포트 5246을 통해 13:11:44에 CAPWAP 에코 요청을 생성했음을 확인합니다.

WLC가 성공적으로 패킷을 수신하고 요청을 처리한 다음 해당 에코 응답을 즉시 생성했습니다. CAPWAP 제어 채널은 DTLS 암호화를 사용하여 보호되므로 응답은 패킷 캡처에서 암호화된 애플리케이션 데이터로 표시됩니다.



No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cz	Total Length	Info
9337	2026-07-19 13:11:44.937939	192.168.100.123	10.105.60.132	DTLSv...	...	0xc0	...	...	...	93	Application Data
9338	2026-07-19 13:11:44.937939	192.168.100.123	10.105.60.132	CAPWA...	...	0xc0	...	...	...	52	CAPWAP-Control - Echo Request
9339	2026-07-19 13:11:44.937939	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	...	...	80	Application Data
9340	2026-07-19 13:11:44.937939	10.105.60.132	192.168.100.123	DTLSv...	...	0xc0	...	...	...	100	Application Data
9755	2026-07-19 13:11:50.174978	10.84.63.223	255.255.255.255	CAPWA...	...	0xc0	...	...	...	426,348	CAPWAP-Control - Discovery Request [Malformed Packet]

스위치 패킷 확인

스위치 패킷 캡처는 암호화된 CAPWAP 제어 패킷이 WLC에서 성공적으로 수신되어 AP로 전달되

있음을 확인합니다.

ip.addr == 192.168.100.123 && capwap											
Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ci	Total Length	At	Id
2026-07-19 13:11:40.004710	10.105.60.132	192.168.100.123	DTLSv...	...	...	0xc0	...	...	93	...	...
2026-07-19 13:11:46.605395	192.168.100.123	10.105.60.132	DTLSv...	...	...	0xc0	...	...	93	...	...
2026-07-19 13:11:46.605419	192.168.100.123	10.105.60.132	DTLSv...	...	...	0xc0	...	...	100	...	...
2026-07-19 13:11:46.605965	10.105.60.132	192.168.100.123	DTLSv...	...	...	0xc0	...	...	100	...	...
2026-07-19 13:11:46.605994	10.105.60.132	192.168.100.123	DTLSv...	...	...	0xc0	...	...	100	...	...

CAPWAP 데이터 킵얼라이브 검증(UDP 포트 5247)

AP는 CAPWAP 데이터 터널의 상태를 확인하기 위해 UDP 포트 5247을 통해 CAPWAP 데이터 킵얼라이브 패킷을 주기적으로 전송합니다.

13:11:44에 AP는 WLC를 향해 데이터 킵얼라이브 패킷을 전송했습니다. WLC가 성공적으로 패킷을 수신하고 즉시 해당 keepalive 응답으로 응답했습니다.

이러한 성공적인 교환을 통해 CAPWAP 데이터 경로가 작동 상태를 유지하고 AP와 WLC 간의 양방향 통신이 정상적으로 작동하고 있음을 확인할 수 있습니다

capwap.keep_alive											
Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ci	Total Length	At	Id
2026-07-19 13:11:44.915937	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:10:44.915937	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:14.925946	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:14.925946	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:14.926938	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:14.926938	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:44.936948	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:44.936948	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...

스위치 패킷 확인

스위치 패킷 캡처는 CAPWAP 데이터 킵얼라이브 패킷이 중단 없이 AP와 WLC 간에 성공적으로 전달되었는지 추가로 확인합니다.

관찰된 패킷 흐름에서는 다음을 확인합니다.

- 데이터 킵얼라이브 패킷이 WLC에 성공적으로 도달했습니다.
- WLC에서 예상 keepalive 응답을 생성했습니다.
- 스위치가 응답을 다시 AP에 전달했습니다.
- 전달 경로 전체에서 패킷 손실이 발생하지 않았습니다.

capwap.keep_alive											
Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Ci	Total Length	At	Id
2026-07-19 13:11:16.593732	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:16.593752	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:16.594302	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:16.594321	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:46.604354	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:46.604372	192.168.100.123	10.105.60.132	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:46.604802	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...
2026-07-19 13:11:46.604822	10.105.60.132	192.168.100.123	CAPWA...	...	...	0xc0	...	...	86	...	...

AP 업링크 스위치에서 삭제되는 제어 패킷(UDP 5246)

이 테스트에서는 AP 업링크 스위치에서 CAPWAP 제어 포트(UDP 5246)가 삭제되는 경우 AP의 동작을 보여줍니다.

WLC가 성공적으로 요청을 처리하고 응답하더라도 CAPWAP 제어 패킷이 AP에 도달하지 못할 경우 AP, WLC 및 네트워크 동작을 검증하는 것이 목적입니다.

이 시나리오에서:

- AP가 WLC를 향해 CAPWAP 에코 요청을 계속 전송합니다.
- WLC는 각 에코 요청을 성공적으로 수신하고 처리합니다.
- WLC에서 해당 에코 응답을 생성합니다.
- AP 업링크 스위치는 응답을 수신하지만 AP에 다시 전달하지 않습니다.
- AP는 에코 응답을 수신하지 않으므로 결국 최대 재전송 횟수를 초과하고 CAPWAP 상태 시스템을 다시 시작합니다.

AP 디버그 분석

12:11:55.4568에서 AP는 UDP 포트 5246을 통해 WLC로 CAPWAP 에코 요청을 전송했습니다.

에코 요청: 보내기 횟수 0

일반적인 작업 시나리오와 달리 에코 응답이 수신되지 않았습니다. 따라서 AP는 기본 CAPWAP 타이머에 따라 재전송을 시작했습니다.

이러한 재전송은 다음과 같은 타임스탬프에 발생했습니다.

Time	이벤트
12:12:00.2587	재전송 수 = 1
12:12:03.2599	재전송 수 = 2
12:12:06.2610	재전송 수 = 3
12:12:09.2624	재전송 수 = 4

Time	이벤트
12:12:12.2637	재전송 수 = 5

다섯 번째 재전송이 실패한 후 AP는 CAPWAP 제어 세션에 연결할 수 없다고 선언했습니다.

AP는 12:12:15.2647에 다음과 같이 보고했습니다.

최대 재전송 수가 초과되어 DISCOVER 모드로 돌아갑니다.

그 직후 AP는 CAPWAP 상태 머신을 재시작하여 새로운 검색 프로세스를 시작했습니다.

```
[*07/17/2026 12:11:54.2577] [RX]KEEPALIVE: Session ID 4068929293, Next scheduled for TX in 30 sec
[*07/17/2026 12:11:54.2577] [RX]KEEPALIVE: RoundTripTime=0.001 sec
[*07/17/2026 12:11:55.4568] Echo Request: Send count 0
[*07/17/2026 12:11:55.4568] [TX]Echo Request: Sent 1 Lost 269
[*07/17/2026 12:12:00.2587] Re-Tx Count=1, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:03.2599] Re-Tx Count=2, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:06.2610] Re-Tx Count=3, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:09.2624] Re-Tx Count=4, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:12.2637] Re-Tx Count=5, Max Re-Tx Value=5, SendSeqNum=63, NumofPendingMsgs=3
[*07/17/2026 12:12:15.2647] Max retransmission count exceeded, going back to DISCOVER mode.
[*07/17/2026 12:12:15.2647] Failed to reach capwap down with retransmission 3 times
```

WLC RA 추적은 컨트롤러에서 처리 문제가 발생하지 않았음을 확인합니다.

12:11:58.731835712에 WLC가 AP에서 전송한 CAPWAP 에코 요청을 성공적으로 수신했습니다. 이러한 로그는 WLC가 요청을 성공적으로 처리하고 적절한 응답을 생성했음을 보여줍니다. 나중에 12:12:19.802183814에 WLC가 AP에서 DTLS Close Notify를 수신했습니다. AP가 컨트롤러에서 전송한 에코 응답을 수신하지 못했기 때문에 연결이 끊겼습니다. 결과적으로 WLC는 DTLS 세션을 종료하고 AP 연결 해제를 기록했습니다.

<#root>

```
2026/07/17 12:12:19.802274790 {wncd_x_R0-1}{2}: [ewlc-dtls-sess] [16522]: (info):
```

```
Remote Host: 192.168.100.120[5256] MAC: 889c.ad26.ea00 dtls session closed
```

```
2026/07/17 12:12:19.802279648 {wncd_x_R0-1}{2}: [ewlc-infra-capwap-dgram] [16522]: (debug): dgram handl
2026/07/17 12:12:19.802317470 {wncd_x_R0-1}{2}: [ewlc-capwapmsg-sess] [16522]: (debug): Encrypted DTLS
2026/07/17 12:12:19.802321202 {wncd_x_R0-1}{2}: [capwapac-smgr-srvr] [16522]: (debug): Mac: 889c.ad26.e
2026/07/17 12:12:19.802376588 {wncd_x_R0-1}{2}: [ap-join-info-db] [16522]: (note): MAC: 889c.ad26.ea00
```

```
AP disconnect initiated. Name : AP12, Ethernet mac : e44e.2d2c.3d0c, Reason: DTLS close alert from peer,
```

<#root>

VK-WLC#show wireless stats ap history | i AP12

```
AP12          889c.ad26.ea00  Joined    07/17/26 12:24:18  NA
AP12          889c.ad26.ea00  Disjoined 07/17/26 12:12:19  NA
AP12          889c.ad26.ea00  Joined    07/17/26 12:09:25  NA
```

AP12 889c.ad26.ea00 Disjoined 07/17/26 12:08:33 NA

Heart be

Monitoring > Wireless > AP Statistics

General Join Statistics AFC Statistics URWB

Clear

ClearAll



Total APs : 4

	AP Name	AP Model	Status	IP Address	Base Radio MAC	Ethernet MAC	Last Reboot Reason (Reported by AP)	Last Disconnect Reason
☐	AP6849.9259.08D0	CW9164I-ROW	⬇	10.105.60.227	10a8.29cf.e540	6849.9259.08d0	No reboot reason	Heart beat timer expiry
☐	Training-AP	C9105AXI-D	⬇	10.105.60.91	6cd6.e32d.f640	6cd6.e336.e138	No reboot reason	AP Auth Failure
☐	AP12	C9130AXI-D	⬇	192.168.100.86	889c.ad26.ea00	e44e.2d2c.3d0c	No reboot reason	Heart beat timer expiry
☐	AP8C88.814F.04E0	CW9178I	⬇	192.168.100.87	ecf4.0cc7.1600	8c88.814f.04e0	No reboot reason	Max Retransmission to AP

1 - 4 of 4 Join Statistics

WLC EPC는 다음을 확인합니다.

- 동일한 타임스탬프에서 CAPWAP 에코 요청이 WLC에 성공적으로 도달했습니다.
- WLC에서 암호화된 CAPWAP 에코 응답을 생성했습니다.
- CAPWAP 제어 트래픽은 DTLS 암호화에 의해 보호되므로 응답은 Application Data로 표시됩니다.

따라서 EPC는 컨트롤러가 성공적으로 응답을 전송했음을 확인합니다. 그러면 문제의 원인인 WLC가 제거됩니다.

48740	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	DTLSv...	0xc0	93	Application Data
48741	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	CAPWA...	0xc0	52	CAPWAP-Control - Echo Request
48742	2026-07-17 12:11:58.731956	10.105.60.132	192.168.100.120	DTLSv...	0xc0	80	Application Data
48743	2026-07-17 12:11:58.731956	10.105.60.132	192.168.100.120	DTLSv...	0xc0	100	Application Data

_ws.col.info == "CAPWAP-Control - Echo Request"

Packet details

Regular Expression

echo

Options:

Narrow & Wide

Case sensitive

Backwards

Multiple occurrences

No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ci	Total Length	At	Id	Info
11212	2026-07-17 12:00:47.679957	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
22807	2026-07-17 12:02:55.731956	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
48741	2026-07-17 12:11:58.730949	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
49001	2026-07-17 12:12:01.732948	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
49292	2026-07-17 12:12:04.733955	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
49485	2026-07-17 12:12:07.734947	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
49695	2026-07-17 12:12:10.735954	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request
49972	2026-07-17 12:12:13.736961	192.168.100.120	10.105.60.132	CAPWA			0xc0	--		52			CAPWAP-Control - Echo Request

AP 업링크 스위치에서 수집한 패킷 캡처는 최종 증거를 제공합니다.

이 캡처를 통해 다음을 확인할 수 있습니다.

- 스위치가 WLC에서 전송한 암호화된 에코 응답을 성공적으로 수신했습니다.
- 이 응답은 DTLS 암호화로 인해 예상되는 애플리케이션 데이터로 표시됩니다.
- 응답이 AP로 전달되지 않았습니다.

그 이유는 다음과 같습니다.

- AP가 CAPWAP 에코 응답을 받지 못했습니다.
- AP가 에코 요청을 계속 재전송했습니다.
- 재전송 카운터가 결국 구성된 임계값을 초과했습니다.
- AP가 CAPWAP 상태 시스템을 다시 시작했습니다.

패킷 캡처는 CAPWAP 제어 트래픽이 중단된 지점으로서 스위치를 명확하게 식별합니다

ip.addr == 192.168.100.120 && capwap													
No.	Time	Source	Destination	Protocol	ID	Pr	Differen	Idi	Ci	Total Length	At	Id	Info
5895	2026-07-17 12:11:50.865681	10.197.34.153	255.255.255.255	CAPWA	--	--	0xc0	--	--	370,292			CAPWAP-Control - Discovery Request [Malformed Packet]
5899	2026-07-17 12:11:50.865752	10.197.34.153	255.255.255.255	CAPWA	--	--	0xc0	--	--	370,292			CAPWAP-Control - Discovery Request [Malformed Packet]
6568	2026-07-17 12:11:58.119507	192.168.100.120	10.105.60.132	DTLSv			0xc0	--	--	1469			Application Data
6569	2026-07-17 12:11:58.119553	192.168.100.120	10.105.60.132	DTLSv			0xc0	--	--	1469			Application Data
6572	2026-07-17 12:11:58.120206	10.105.60.132	192.168.100.120	DTLSv			0xc0	--	--	1469			Application Data
6663	2026-07-17 12:11:58.401490	10.84.63.223	255.255.255.255	CAPWA	--	--	0xc0	--	--	426,348			CAPWAP-Control - Discovery Request [Malformed Packet]

AP 업링크 스위치에서 삭제되는 CAPWAP 데이터 포트(UDP 5247)

이 테스트는 CAPWAP 제어 포트(UDP 5246)가 작동 상태를 유지하는 동안 AP 업링크 스위치에서 CAPWAP 데이터 포트(UDP 5247)가 삭제될 때 AP 동작을 검증합니다.

이전 시나리오와 달리 AP는 UDP 포트 5246을 통해 CAPWAP 에코 메시지를 성공적으로 교환하여 WLC와의 CAPWAP 제어 연결을 계속 유지합니다. 그러나 CAPWAP 데이터 킵얼라이브 패킷이 왕복 경로를 완료할 수 없으므로 AP는 결국 CAPWAP 데이터 경로를 도달 불가로 선언하고 CAPWAP 재시작을 시작합니다.

AP 디버그 로그는 테스트 동안 CAPWAP 제어 채널이 계속 작동함을 확인합니다.

캡처를 시작할 때 UDP 포트 5246을 통해 전송된 CAPWAP 에코 요청이 WLC에서 유효한 에코 응답을 계속 받아 중단 없는 컨트롤 플레인 통신을 확인했습니다.

그러나 14:30:15에 AP가 UDP 포트 5247을 통해 CAPWAP 데이터 킵얼라이브 패킷을 전송했습니다. 해당 데이터 킵얼라이브 응답이 수신되지 않았기 때문에 AP가 재시도 메커니즘을 시작했습니다. 다음 타임스탬프에서 재전송을 확인할 수 있습니다.

타임스탬프	이벤트
14:30:15	초기 데이터 킵얼라이브 전송
14:30:19	다시 시도 1
14:30:25	재시도 2
14:30:37	재시도 3
14:30:49	재시도 4
14:31:01	다시 시도 5
14:31:13	최종 재시도

이 기간 동안 CAPWAP 에코 응답이 계속 수신되었지만 AP가 데이터 킵얼라이브 패킷에 대한 응답을 받지 못했습니다. 재시도 시도가 모두 종료된 후 AP는 암호화되지 않은 데이터 킵얼라이브 시간 초과를 보고하고 CAPWAP 재시작을 시작했습니다. 약 14:31:16에 AP는 기존 CAPWAP 세션을 종료하고 검색 프로세스로 돌아왔습니다.

```
AP12#[*07/19/2026 14:30:15.9995] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:15.9995] [TX]KEEPALIVE: Schedule for Retransmit in 3 sec sec_drop_count=0
[*07/19/2026 14:30:15.9996] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 14:30:19.0002] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:19.0002] [TX]KEEPALIVE: Schedule for Retransmit in 6 sec sec_drop_count=0
[*07/19/2026 14:30:19.0003] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 14:30:25.0023] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:25.0024] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:30:25.0024] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 14:30:37.0066] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:37.0066] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:30:37.0067] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 14:30:49.0109] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:30:49.0109] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:30:49.0109] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
```

```
[*07/19/2026 14:31:01.0151] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:31:01.0151] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:31:01.0152] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 14:31:13.0195] [TX]KEEPALIVE: Send to 10.105.60.132-5247
[*07/19/2026 14:31:13.0195] [TX]KEEPALIVE: Schedule for Retransmit in 12 sec sec_drop_count=0
[*07/19/2026 14:31:13.0196] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 14:31:16.0207] Warning, unencrypted data keepalive failed
[*07/19/2026 14:31:16.0207] Going to restart CAPWAP (reason : data keepalive not received)...
```

CAPWAP 데이터 채널의 경우 추적은 컨트롤러가 예상 Data Keepalive 패킷을 수신하지 못했음을 나타냅니다. 결국 AP가 Data Keepalive 실패를 선언한 후 WLC가 DTLS 세션 종료 및 AP 연결 해제 이벤트를 기록했습니다. RA에서 관찰된 순서에 따라 Data Keepalive 시간 초과로 인해 AP가 자발적으로 연결을 끊을 때까지 컨트롤러가 작동 중임을 확인합니다.

AP 이더넷 mac을 사용한 RA 추적:

<#root>

```
2026/07/19 14:31:16.842212773 {fman_rp_R0-0}{2}: [source] [20448]: (debug): ipc(mqipc/wncd_2/wncd-fmrp)
2026/07/19 14:31:16.842250177 {wncd_x_R0-2}{2}: [errmsg] [16638]: (note): %CAPWAPAC_SMGR_TRACE_MESSAGE-
2026/07/19 14:31:16.842251233 {wncd_x_R0-2}{2}: [capwapac-smgr-sess-fsm] [16638]: (note): Mac: 889c.ad26.ea00
```

Last Data Keep Alive Packet received 90 seconds ago.

```
2026/07/19 14:31:16.843318439 {wncmgrd_R0-0}{2}: [loadbalance-algo] [16262]: (note): Algo counter decre
2026/07/19 14:31:16.843318599 {wncd_x_R0-2}{2}: [wsa-core] [16638]: (debug): WSA AP EVT Create Populate
2026/07/19 14:31:16.843320409 {wncd_x_R0-2}{2}: [wsa-core] [16638]: (debug): WSA AP EVT Create Populate
```

DISJOIN - AP Mac:889c.ad26.ea00 , new ap disconnect reason 'DTLS close alert from peer' (26)

무선 MAC으로 RA 추적:

<#root>

```
2026/07/19 14:31:16.737070835 {wncd_x_R0-2}{2}: [capwapac-smgr-sess] [16638]: (debug): Mac: 889c.ad26.ea00
2026/07/19 14:31:16.737072831 {wncd_x_R0-2}{2}: [capwapac-smgr-srvr] [16638]: (debug): Mac: 889c.ad26.ea00
2026/07/19 14:31:16.737076419 {wncd_x_R0-2}{2}: [msc-fsm] [16638]: (debug): @msc_event {"entity":"/capw
2026/07/19 14:31:16.737078137 {wncd_x_R0-2}{2}: [msc-fsm] [16638]: (debug): @msc_event {"entity":"/capw
2026/07/19 14:31:16.841870791 {wncd_x_R0-2}{2}: [ap-join-info-db] [16638]: (note): MAC: 889c.ad26.ea00
```

AP disconnect initiated. Name : AP12, Ethernet mac : e44e.2d2c.3d0c, Reason: DTLS close alert from peer,

```
2026/07/19 14:31:16.841890831 {wncd_x_R0-2}{2}: [capwapac-smgr-srvr] [16638]: (debug): MAC: 889c.ad26.ea00
```

WLC에서 수집된 EPC는 컨트롤러측 패킷 처리를 검증합니다. 캡처는 CAPWAP 제어 패킷이 테스트 동안 계속 성공적으로 교환되었지만 wlc에서 수신된 데이터 킵얼라이브 패킷이 없음을 확인합니다. 이 관찰은 AP 디버그 로그와 일치하며 제어 채널이 활성 상태임에도 불구하고 데이터 킵얼라이브 메커니즘이 실패했음을 보여 줍니다.

Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cz	Total Length	Al	Id	Info
11827	2026-07-19 14:30:13.475973	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	85			Application Data
11828	2026-07-19 14:30:13.476965	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	117			Application Data
11829	2026-07-19 14:30:13.476965	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	76			CAPWAP-Control - WTP Event Request
11830	2026-07-19 14:30:13.476965	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	65			Application Data
11831	2026-07-19 14:30:13.476965	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	85			Application Data
11928	2026-07-19 14:30:16.714959	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	1469			Application Data
11929	2026-07-19 14:30:16.714959	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	1428			CAPWAP-Control - WTP Event Request [Malformed Packet]
11930	2026-07-19 14:30:16.715951	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	1449			Application Data
11931	2026-07-19 14:30:16.715951	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	1469			Application Data
11990	2026-07-19 14:30:18.024992	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	437			Application Data
11991	2026-07-19 14:30:18.024992	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	396			CAPWAP-Control - WTP Event Request
11992	2026-07-19 14:30:18.025984	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	65			Application Data
11993	2026-07-19 14:30:18.025984	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	85			Application Data
11994	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	437			Application Data
11995	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	396			CAPWAP-Control - WTP Event Request
11996	2026-07-19 14:30:18.028990	192.168.100.123	10.105.60.132	DTLSv..	--	0xc0	--	--	65			Application Data
11997	2026-07-19 14:30:18.028990	10.105.60.132	192.168.100.123	DTLSv..	--	0xc0	--	--	85			Application Data
12034	2026-07-19 14:30:18.236987	10.132.179.233	255.255.255.255	CAPWA..	--	0xc0	--	--	378,300			CAPWAP-Control - Discovery Request [Malformed Packet]
12036	2026-07-19 14:30:18.236987	10.132.179.233	255.255.255.255	CAPWA..	--	0xc0	--	--	378,300			CAPWAP-Control - Discovery Request [Malformed Packet]

스위치:

AP 업링크 스위치에서 수집된 패킷 캡처는 패킷이 스위치에 존재하지만 wlc로 전달되지 않았음을 보여줍니다

Time	Source	Destination	Protocol	ID	Pr	Differen	Id	Cz	Total Length	Al	Id	Info
3300	2026-07-19 14:20:40.332207	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
3303	2026-07-19 14:28:48.332827	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
3304	2026-07-19 14:28:48.332844	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5336	2026-07-19 14:29:18.342564	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5337	2026-07-19 14:29:18.342586	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5340	2026-07-19 14:29:18.343037	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
5341	2026-07-19 14:29:18.343092	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8573	2026-07-19 14:29:48.353254	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8574	2026-07-19 14:29:48.353322	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8577	2026-07-19 14:29:48.353998	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
8578	2026-07-19 14:29:48.354018	10.105.60.132	192.168.100.123	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
10376	2026-07-19 14:30:18.363535	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
10534	2026-07-19 14:30:21.364195	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
10837	2026-07-19 14:30:27.366201	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
11465	2026-07-19 14:30:39.370239	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
12141	2026-07-19 14:30:51.374346	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
12959	2026-07-19 14:31:03.378437	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
13620	2026-07-19 14:31:15.382538	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
15834	2026-07-19 14:31:43.032731	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
16474	2026-07-19 14:31:46.000877	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
16886	2026-07-19 14:31:52.003518	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
17809	2026-07-19 14:32:04.007609	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]
18576	2026-07-19 14:32:16.013892	192.168.100.123	10.105.60.132	CAPWA..	--	0xc0	--	--	86			CAPWAP-Data Keep-Alive [Malformed Packet]

CAPWAP 데이터 킵얼라이브 비활성화

이 기능은 Cisco 버그 ID CSCvs에서 [도입되었습니다66015](#)

이 기능은 이러한 시나리오의 트러블슈팅에 유용합니다.

1. AP 연결 끊기 문제 해결: capwap 데이터 킵얼라이브를 비활성화한 후 capwap 제어 킵얼라이브로 인해 AP가 여전히 연결 끊어지고 있는지 확인하고 AP 킵얼라이브 연결 해제에 근본 원인을 파악할 수 있습니다.
2. capwap data-keepalive가 삭제되는 이유를 확인할 때까지 이를 해결하는 방법으로 capwap

data-keepalive로 인한 연결 해제를 방지합니다.

3. 낮은 처리량으로 WAN 링크를 통해 연결된 브랜치 폴렉스 구축의 스니퍼 AP. AP 중 하나를 스니퍼 모드로 구성하는 OTA 패킷 캡처를 수집하려는 경우, 모든 캡처된 패킷은 capwap 데이터 포트를 사용하여 WAN 링크를 통해 WLC로 전송됩니다. 이렇게 하면 WAN 링크가 마비되고 전체 브랜치에 영향을 미칩니다.
4. 스니퍼 모드에서 AP에 대한 capwap 데이터 킵얼라이브를 비활성화하고 해당 콘크리트 AP에서 capwap 데이터 패킷을 삭제하기 위해 브랜치에 ACL을 생성하면 capwap 제어가 잘 되므로 AP가 연결된 상태로 유지되므로 패킷 캡처가 포함된 WAN 링크를 과도하게 사용하지 않고도 AP switchport에서 OTA를 수집할 수 있습니다.

9800 WLC에서 COS-AP 데이터 킵얼라이브 활성화/비활성화를 트리거합니다. 기본적으로 WLC 및 AP에서 데이터 킵얼라이브가 활성화되어 있습니다.

WLC 명령:

- 1) "Unencrypted Data Keep Alive" 문자열로 상태를 표시합니다.

```
show ap config general
```

- 2) ap 이름으로 데이터 킵얼라이브 활성화/비활성화

```
ap name AP-NAME keepalive  
ap name AP-NAME no keepalive
```

AP 자체에서 COS-AP 데이터 킵얼라이브 활성화/비활성화 트리거. 기본적으로 AP의 데이터 킵얼라이브는 활성화되어 있습니다.

AP 명령:

- 1) "Unencrypted Data Keep Alive" 문자열로 상태를 표시합니다.

```
show capwap client config
```

- 2) AP에서 데이터 킵얼라이브 활성화/비활성화

```
capwap ap unencrypted_data_keepalive enable
```

```
capwap ap unencrypted_data_keepalive disable
```

예를 들면 다음과 같습니다.

ap 수준에서 keepalive 검사를 비활성화했습니다.

```
AP12#capwap ap unencrypted_data_keepalive disable
```

```
<#root>
```

```
AP12#show capwap client configuration
```

```
AdminState           : ADMIN_ENABLED(1)
Name                  : AP12
Location              : default location
Primary controller name : VK-WLC
Primary controller IP   : 10.105.60.132
Secondary controller name : 9800-demo
Secondary controller IP : 10.106.39.156
Tertiary controller name :
ssh status            : Enabled
ApMode                 : Local
ApSubMode              : Not Configured
Link-Encryption        : Disabled
```

```
Unencrypted Data Keep Alive : Disabled
```

```
OfficeExtend AP      : Disabled
Discovery Timer       : 10
```

AP 디버깅:

ap debug에서는 AP와 wlc 간에 데이터 keepalive 패킷 교환이 발생하지 않음을 볼 수 있으며, 제어 패킷 교환만 볼 수 있습니다.

```
AP12#debug capwap 클라이언트 keepalive
```

```
AP12#[*07/19/2026 15:24:33.4087] Echo Request: Send count 0
[*07/19/2026 15:24:33.4087] [TX]Echo Request: Sent to 10.105.60.132
[*07/19/2026 15:24:33.4112] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:24:34.0006] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 15:25:34.0032] Echo Request: Send count 1
```

```
[*07/19/2026 15:25:34.0032] [TX]Echo Request: Sent 2 Lost 2
[*07/19/2026 15:25:34.0056] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:25:34.0006] [RX]Echo Response from 10.105.60.132 RttCount 2
[*07/19/2026 15:27:34.0327] Echo Request: Send count 2
[*07/19/2026 15:27:34.0327] [TX]Echo Request: Sent 3 Lost 2
[*07/19/2026 15:27:34.0347] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:27:34.0004] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 15:28:34.0025] Echo Request: Send count 3
[*07/19/2026 15:28:34.0025] [TX]Echo Request: Sent 4 Lost 2
[*07/19/2026 15:28:34.0050] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:28:34.0022] [RX]Echo Response from 10.105.60.132 RttCount 2
AP12#[*07/19/2026 15:29:43.5772] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
[*07/19/2026 15:30:04.0140] Echo Request: Send count 4
[*07/19/2026 15:30:04.0140] [TX]Echo Request: Sent 5 Lost 2
[*07/19/2026 15:30:04.0164] [RX]Echo Response from 10.105.60.132
[*07/19/2026 15:30:04.0011] [RX]Echo Response from 10.105.60.132 RttCount 1
[*07/19/2026 15:30:27.7695] capwap_ap_upstream_send ip: 192.168.100.123, port: 5272 => ip: 10.105.60.132
```

데이터 킵얼라이브 패킷이 삭제되었지만 데이터 킵얼라이브 검사를 비활성화했으므로 킵얼라이브 패킷 삭제의 영향을 받지 않고 AP가 wlc에서 안정적으로 유지되는 것을 확인할 수 있습니다.

Monitoring > Wireless > AP Statistics

General Join Statistics AFC Statistics URWB

Total APs : 1

Misconfigured APs

Tag : 0

Country Code : 0

LSC Falback : 0

URWB : 0

License Non-Compliance ⓘ

Non Compliant APs : 0



Multiple APs can be configured at once from Bulk AP Provisioning feature

AP Name	AP Model	Admin Status	Up Time	WLC Association Uptime	IP Address	AP Radio MAC	Ethernet MAC	Operation Status
AP12	C9130AXI-D	✓	0 days 3 hrs 58 mins 7 secs	0 days 0 hrs 12 mins 25 secs	192.168.100.123	889c.ad26.ea00	e44e.2d2c.3d0c	Registered

1 - 1 of 1 items

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.